

УТВЕРЖДАЮ
Декан факультета

(подпись) Страхов С. Ю.
ФИО
«___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Направление/специальность подготовки	09.04.04 Программная инженерия
Специализация/профиль/программа подготовки	Процессы и методы разработки программных продуктов
Уровень высшего образования	Магистратура
Форма обучения	Заочная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
2	3	3	108	8	4	0	4	100	0	0	100	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

**РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)**

09.04.04 Программная инженерия

год набора группы: 2024

Программу составил:

Кафедра И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ
Стукалова Анна Сергеевна, старший преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ**

Заведующий кафедрой Страхов С.Ю., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-5 — способность разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ПСК-2.3 — способность организовывать разработку программного обеспечения для анализа, распознавания и обработки информации
ПСК-2.4 — способность организовывать разработку программного обеспечения для систем цифровой обработки сигналов

Формированию компетенций служит достижение следующих результатов образования:

ОПК-5

знания:

знать физико-математический аппарат для решения задач кодирования и криптографии;

знать основы передачи информации, понимать принцип действия алгоритмов кодирования и криптографии;

знать программное и аппаратное обеспечение информационных и автоматизированных систем;

умения:

уметь создавать специализированное программно-математическое обеспечение для исследования вопросов кодирования информации при передаче по линиям связи;

навыки:

владеть методами анализа, трансформации, визуализации исследуемой информации и применять знания и умения для получения требуемого результата.

ПСК-2.3

знания:

знать принципы обработки информации;

знать современные информационные технологии и основные подходы к защите информации при передаче по каналам связи;

умения:

уметь определять круг задач, решаемых с помощью исследуемых методов и алгоритмов;

уметь применять физико-математический аппарат для решения задач кодирования и криптографии;

уметь собирать и анализировать информацию для формирования исходных данных при проектировании линий и каналов связи;

навыки:

владеть методами анализа, трансформации, визуализации исследуемой информации.

ПСК-2.4

знания:

знать основы передачи информации, включая современные беспроводные методы, понимать принцип действия алгоритмов кодирования и криптографии, включая алгоритмы квантовой криптографии и технологии блокчейн;

умения:

уметь использовать современные языки программирования для программной реализации алгоритмов кодирования и криптографии;

навыки:

иметь навык реализации алгоритмов кодирования и сжатия данных;

иметь навык реализации протоколов защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.04.04 Программная инженерия*.

Содержание дисциплины является логическим продолжением дисциплин: **МЕТОДОЛОГИЯ ПРОГРАММНОЙ ИНЖЕНЕРИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте
- ПСК-2.1 — Способен выполнить постановку новых задач анализа и синтеза новых проектных решений

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %		
				ВСЕГО	Лекции	Практические занятия		ОПК-5	ПСК-2.3	ПСК-2.4
2	3	Раздел 1. Элементы теории информации и информационной техники. Раздел 1. Элементы теории информации и информационной техники. 1.1 Теоретические основы информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах. 1.2 Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS, RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиоинтерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	24	2	1	1	22	20	20	20
2	3	Раздел 2. Кодирование данных. 2.1 Общие понятия и определения. Цели кодирования. Принципы помехоустойчивого кодирования. 2.2 Блочные коды. Простейшее кодирование, прямоугольные коды, код Хэмминга. Технические средства кодирования и декодирования. 2.3 Циклические коды. Математические основы и принципы формирования. Технические средства кодирования и декодирования.	26	2	1	1	24	20	30	30
2	3	Раздел 3. Сжатие данных. 3.1 Общие понятия и определения. Цели сжатия данных. Принципы построения алгоритмов сжатия данных. 3.2 Алгоритмы сжатия без потерь. Кодирование длин серий. Сжатие со словарем. Статистические методы сжатия. Область применения и особенности. Метод Хаффмана. Метод арифметического кодирования. 3.3 Алгоритмы сжатия с потерями. Принципы дискретно-косинусного преобразования. Вейвлет- алгоритм. Область применения и особенности.	26	2	1	1	24	30	30	30
2	3	Раздел 4. Элементы криптографии. Раздел 4. Элементы криптографии. 4.1 Общие понятия и определения. Цели криптографии. Принципы построения алгоритмов криптографии. Обзор существующих методов криптографии. 4.2 Алгоритмы криптографии с симметричным ключом. Математические основы. Технические средства. Область применения и особенности. 4.3 Алгоритмы криптографии с открытым ключом. Математические основы. Технические средства. Область применения и особенности. Квантовая криптография. Алгоритм BB84. 4.4 Алгоритмы электронной подписи. Математические основы. Технические средства. Область применения и особенности. 4.5 Прочие криптографические протоколы: аутентификации, целостности, анонимности. Хеширование, алгоритм Фейге-Фиата-Шамира, Kerberos, биометрические технологии идентификации.	32	2	1	1	30	30	20	20
Всего за 3 семестр			108	8	4	4	100	100	100	100
Всего по дисциплине			108	8	4	4	100	100	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Элементы теории информации и информационной техники.	Пропускная способность канала в зависимости от метода физического кодирования. Расчет пропускной способности.	1
2	Раздел 2. Кодирование данных.	Повторение принципов построения блочных кодов. Код Хэмминга для исправления однократных ошибок. Повторение кода Хэмминга для исправления двукратных ошибок.	1
3	Раздел 3. Сжатие данных.	Сжатие последовательности методом Хаффмана. Работа в малых группах. Реализация алгоритма Хаффмана по заданному варианту с использованием пакета прикладных программ, построение дерева	1

		решений при помощи инструментов визуализации, расчет эффективности алгоритма для заданного случая, сдача отчета в электронном виде. Арифметическое кодирование. Реализация алгоритма в среде программирования либо в MS Excel, расчет эффективности алгоритма для заданного случая, сдача отчета в электронном виде	
4	Раздел 4. Элементы криптографии.	Алгоритм Луна. Способы создания случайных и псевдослучайных последовательностей. Алгоритмы гаммирования, Блум-Блум-Шуба, RC4/	1
Всего за 3 семестр			4

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Элементы теории информации и информационной техники.	Повторение и осмысление сведений об основных элементах теории информации и информационной техники. Элементы теории информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах. Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS. RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиоинтерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	22
2	Раздел 2. Кодирование данных.	Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации. Исследование реализации сверточного кода с использованием пакета специализированного ПО.	24
3	Раздел 3. Сжатие данных.	Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных. Исследование вариантов реализации алгоритмов Хаффмана, арифметического кодирования, RLE, LZ78 с применением средств программирования. Исследование алгоритма JPEG.	24
4	Раздел 4. Элементы криптографии.	Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности. Исследование разных типов алгоритмов хеширования. Обзор в виде таблицы сравнения.	30
Всего за 3 семестр			100

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3			ИПЗ		ИПЗ	ДР	ИПЗ		ИПЗ	ДР	ИПЗ		ИПЗ			ДР	Тест, диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- ИПЗ – индивидуальное практическое задание;
- Тест – тест;
- диф. зач. – дифференцированный зачет.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- индивидуальное практическое задание;
- тест.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. А. М. Голиков. . Кодирование и шифрование информации в системах связи. Томск: ТУСУР, 2016, эл. рес.
3. В. Д. Вавилов, С. П. Тимошенко, А. С. Тимошенко. . Микросистемные датчики физических величин. М.: Техносфера, 2018, 40 экз.
4. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
5. Е. Г. Лебедько. . Теоретические основы передачи информации. Санкт-Петербург: Лань, 2022, эл. рес.
6. Е. Ф. Берёзкин. . Основы теории информации и кодирования. СПб.: Лань, 2019, 9 экз.
7. И. В. Черпаков. . Теоретические основы информатики. Москва: Юрайт, 2017, эл. рес.
8. Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование. Москва: Юрайт, 2020, эл. рес.
9. М. Вернер. . Основы кодирования. М.: Техносфера, 2004, 50 экз.
10. М. Ю. Рыгов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации. Старый Оскол: ТНТ, 2021, эл. рес.
11. С. А. Курицын. . Телекоммуникационные технологии и системы. М.: Академия, 2008, 6 экз.
12. С. А. Ляшева, М. П. Шлеймович, З. Т. Яхина. . Теория информации и кодирования. Казань: КНИТУ-КАИ, 2020, эл. рес.

5.2. Дополнительная литература по дисциплине:

1. Д. Сэломон. . Сжатие данных, изображений и звука. М.: Техносфера, 2004, 3 экз.
2. С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security. М.: БИНОМ, 2007, 3 экз.

5.3. Периодические издания:

1. Научно-методический журнал «Информатизация образования и науки»;
2. Радиотехника – XXI век.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://library.voenmeh.ru> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. <http://e.lanbook.com> — ЭБС Лань;
3. <http://urait.ru> — Образовательная платформа «Юрайт». Для вузов и ссузов..

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. NI Multisim - академическая версия.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. NI Multisim - академическая версия.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.04.04 Программная инженерия*. Дисциплина реализуется на факультете И Информационных и управляющих систем БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ.

Дисциплина нацелена на формирование *компетенций*:

ОПК-5 способность разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

ПСК-2.3 способность организовывать разработку программного обеспечения для анализа, распознавания и обработки информации;

ПСК-2.4 способность организовывать разработку программного обеспечения для систем цифровой обработки сигналов.

Содержание дисциплины охватывает круг вопросов, связанных с основами кодирования, криптографии и передачи информации.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- индивидуальное практическое задание;
- тест.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет 3 з.е., **108 ч**. Программой дисциплины предусмотрены лекционные занятия (**4 ч.**), практические занятия (**4 ч.**), самостоятельная работа студента (**100 ч**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 8 ч. аудиторных занятий, и 100 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Элементы теории информации и информационной техники.		
Повторение и осмысление сведений об основных элементах теории информации и информационной техники. Элементы теории информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах. Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS. RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиоинтерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	<p>Е. Г. Лебедько. . Теоретические основы передачи информации: Санкт-Петербург: Лань, 2022 (все)</p> <p>В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1, 2, 3)</p> <p>И. В. Черпаков. . Теоретические основы информатики: Москва: Юрайт, 2017 (1-3)</p> <p>С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (2, 3)</p> <p>В. Д. Вавилов, С. П. Тимошенко, А. С. Тимошенко. . Микросистемные датчики физических величин: М.: Техносфера, 2018 (все)</p>	22
Итого по разделу 1		22
Раздел 2. Кодирование данных.		
Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации. Исследование реализации сверточного кода с использованием пакета специализированного ПО.	<p>А. М. Голиков. . Кодирование и шифрование информации в системах связи: Томск: ТУСУР, 2016 (все)</p> <p>М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (1, 2, 3)</p>	24

Итого по разделу 2		24
Раздел 3. Сжатие данных.		
Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных. Исследование вариантов реализации алгоритмов Хаффмана, арифметического кодирования, RLE, LZ78 с применением средств программирования. Исследование алгоритма JPEG.	Д. Сэломон. . Сжатие данных, изображений и звука: М.: Техносфера, 2004 (все) Е. Ф. Берёзкин. . Основы теории информации и кодирования: СПб.: Лань, 2019 (все) С. А. Ляшева, М. П. Шлеймович, З. Т. Яхина. . Теория информации и кодирования: Казань: КНИТУ-КАИ, 2020 (все)	24
Итого по разделу 3		24
Раздел 4. Элементы криптографии.		
Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности. Исследование разных типов алгоритмов хеширования. Обзор в виде таблицы сравнения.	М. Ю. Рытов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации: Старый Оскол: ТНТ, 2021 (3-8) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (все) Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (все) Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (все) С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security: М.: БИНОМ, 2007 (все)	30
Итого по разделу 4		30

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- тест;
- индивидуальное практическое задание;
- дифференцированный зачет.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Тест

Тест включает в себя 10 вопросов. Требуется выбрать один правильный ответ из предложенных. Время выполнения 10 минут. Успешное прохождение теста регистрируется при условии получения не менее 6 правильных ответов. Оценка "хорошо" - не менее 8 правильных ответов. Оценка "отлично" - не менее 9 правильных ответов.

Примеры представлены в УМК в дисциплины.

Индивидуальное практическое задание

Отчет по индивидуальному заданию должен содержать полное решение согласованной с преподавателем задачи.

Примеры заданий и типовые задачи представлены в УМК в дисциплины.

Дифференцированный зачет

Для допуска к зачёту необходимо защитить все лабораторные работы. Оценка дифференцированного зачёта ставится с учётом ответов на вопросы при проведении устного зачета в виде блиц-ответов на заранее выданный список вопросов.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %			НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-5	ПСК-2.3	ПСК-2.4	
2	3	Раздел 1. Элементы теории информации и информационной техники.	24	2	1	1	22	20	20	20	Тест, Индивидуальное практическое задание
2	3	Раздел 2. Кодирование данных.	26	2	1	1	24	20	30	30	Индивидуальное практическое задание, Тест
2	3	Раздел 3. Сжатие данных.	26	2	1	1	24	30	30	30	Индивидуальное практическое задание, Тест
2	3	Раздел 4. Элементы криптографии.	32	2	1	1	30	30	20	20	Индивидуальное практическое задание, Тест
Всего за 3 семестр			108	8	4	4	100	100	100	100	
Всего по дисциплине			108	8	4	4	100	100	100	100	

Критерии оценивания

ОПК-5

- Вопросы открытого типа:*
- № 1 Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 797кГц
- № 2 Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 532 Гц, отношение сигнал/шум 56 Дб
- № 3 Определить ширину спектра в передаваемом сообщении, закодированном АМІ-кодом: 01001100011, если пропускная способность канала составляет 227089 бит/с. Ответ представить в Гц
- № 4 Определить требуемое минимальное расстояние по Хеммингу для исправления 4-кратной ошибки
- № 5 Определить вероятность пропуска ошибки при передаче четырех информационных разрядов кода с контролем четности, если вероятность безошибочной передачи равна 0,9.
- !!!Учесть суммарное количество разрядов кода!
- № 6 Вычислить степень сжатия, если длина исходного сообщения равна 888, длина сжатого - 542
- № 7 Минимальное количество ключей, необходимое для приватного общения группы из 34 пользователей равно
- № 8 Найти пропущенную в номере банковской карты цифру:
- 4460X84553390931
- № 9 Определить значение функции Эйлера для числа 13
- № 10 К симметричным методам относятся:
- Эллиптических кривых
- BB84
- RSA
- Эль-Гамала
- DES
- Диффи-Хеллмана
- AES
- Вопросы закрытого типа:*
- № 1 Определить количество информации в комбинаторной мере для двоичной системы счисления при условии, что передается два сообщения величиной 9 бит и 1 бит
- 512
- 10
- 1024
- 2048
- № 2 Энтропия максимальна, когда вероятность наступления события $p_i =$
- 1
- 0
- 0.5
- 1/i
- № 3 Преобразование давления в электрический сигнал присуще следующему эффекту:

	фотогальваническому пьезоэлектрическому
	Зеебека
	электромагнитной индукции
№ 4	пироэлектрическому Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
	2
	1
	4
№ 5	2^n Разработчик первого алгоритма с открытыми ключами:
	Хеллман
	Шнайер
	Фейстель
	Брассар
№ 6	Шамир Невозможность несанкционированного изменения информации - это
	идентификация
	обеспечение криптостойкости
	аутентификация
	обеспечение конфиденциальности
№ 7	обеспечение целостности Если буквы меняют свои позиции, но сохраняют свои роли, то это:
	шифр подстановки
	шифр Цезаря
	шифр Полибия
№ 8	перестановочное шифрование Является ли следующая последовательность кодов префиксным кодом?
	00
	01
	10
	110
	101
№ 9	Энтропия равна 0, когда вероятность наступления события $p_i = 0$
№ 10	Зашифрованная с помощью афинного шифра (2,1) буква Б русского алфавита (позиции алфавита 0:32) будет определяться символом Г

ПСК-2.3

Вопросы открытого типа:

- № 1 Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 346 Гц, отношение сигнал/шум 24 Дб
- № 2 Определить ширину спектра в передаваемом сообщении при кодировании АМІ_кодом сообщения: 0101010000001111101100, если пропускная способность канала составляет 812703 бит/с. Ответ представить в Гц
- № 3 Определить требуемое минимальное расстояние по Хеммингу для обнаружения 9-кратной ошибки
- № 4 Определить требуемое минимальное расстояние по Хеммингу для обнаружения 12-кратной ошибки и исправления 7-кратной
- № 5 Избыточность кода с 112 информационными и 13 проверочными битами равна
- № 6 Вычислить разрешенную кодовую комбинацию циклического кода для информационной последовательности 1001 и образующего полинома 1011
- № 7 Вычислить степень сжатия, если длина исходного сообщения равна 888, длина сжатого - 542
- № 8 Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц
- № 9 Определить вес кодовой комбинации: 11110000000011
- № 10 Энтропия максимальна, когда вероятность наступления нескольких событий

Вопросы закрытого типа:

- № 1 Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц

542

542000

293764

1084

1084000

- № 2 Самая помехозащищенная линия связи на основе:

коаксиальный кабель

радиолиния

витая пара

волоконно-оптический кабель

беспроводная оптическая линия

- № 3 Какова цель использования генераторов псевдослучайных чисел при поточном шифровании?

формирование открытых ключей

защита информации от всех случайных или преднамеренных изменений

получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа

защита информации от случайных помех при передаче и хранении

сжатие информации

- № 4 Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии:

функцией Диффи-Хеллмана

односторонней функцией

- функцией Эйлера
- № 5 криптографической функцией
Что является особенностью использования режима CBC блочного шифра?
одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст
- сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке
- одинаковые блоки исходного текста преобразуются в одинаковый шифротекст
- этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений
- сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока
- № 6 Какой язык обладает минимальной избыточностью сообщений?
- Язык, в котором только два символа
- Язык, в котором некоторые символы гораздо вероятнее других
- Язык, в котором как можно больше символов
- Язык, в котором все символы равновероятны и могут встречаться в сообщениях независимо друг от друга в любом порядке
- № 7 Для чего предназначен алгоритм Блума-Блюма-Шуба (BBS)?
- для генерации псевдослучайных чисел
- для сжатия информации
- для формирования открытых ключей
- для формирования хеш-кода
- № 8 Кто предложил реализацию совершенно секретной системы, называемую в настоящее время одноразовой лентой или одноразовым блокнотом?
- Шеннон
- Вернам
- Альберти
- Вижнер
- № 9 Какой алгоритм не используется для шифрования?
- AES
- DES
- RSA
- Диффи-Хеллмана
- № 10 Выберите вариант ответа, содержащий только взаимно простые числа:
- 7, 27, 77, 147
- 5, 9, 27, 54
- 3, 7, 25, 38
- 4, 7, 16, 59

- Вопросы открытого типа:*
- № 1 Максимальное значение энтропии источника, который порождает 16 различных символов равно:
- № 2 Как соотносятся коды Фано и Хаффмана для источника с равномерным распределением вероятностей?
- Равны
- В Хаффмана больше символов
- В Фано больше символов
- № 3 Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 614кГц
- № 4 Определить кодовое расстояние по Хеммингу двух кодовых комбинаций: 111000111 и 111110111
- № 5 Вычислить коэффициент сжатия, если длина исходного сообщения равна 356, длина сжатого - 60
- № 6 К симметричным методам относятся:
- Эллиптических кривых
- BB84
- RSA
- Эль-Гамала
- DES
- Диффи-Хеллмана
- AES
- № 7 Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?
- сложение по модулю 2
- нахождение остатка от деления на большое простое число
- замена бит по таблице замен
- перестановка бит
- возведение в степень
- № 8 Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя, пришедший на смену DES:
- № 9 Первый алгоритм семейства LZ со скользящим окном:
- № 10 Сообщения передаются 3-разрядным и 2-разрядным двоичным кодом. Определить количество информации по Хартли, передаваемое двумя сообщениями
- Вопросы закрытого типа:*
- № 1 Каким преимуществом не обладает цифровая система обработки по сравнению с аналоговой:
- Отсутствие проблемы согласования нагрузок
- Малые габариты и потребление
- Высокая точность преобразования
- Высокая стабильность характеристик
- № 2 Какая процедура называется дискретизацией:
- Прореживание отсчетов по времени

	Прореживание отсчетов по частоте
	Преобразование аналоговых отсчетов сигнала в цифровые
№ 3	Взятие мгновенных значений сигнала с заданным периодом Какая процедура называется квантованием:
	Прореживание отсчетов по времени
	Преобразование аналоговых отсчетов сигнала в цифровые
	Взятие мгновенных значений сигнала с заданным периодом
№ 4	Переход из временной области в частотную Сообщения передаются 8-разрядным и 7-разрядным двоичным кодом. Определить количество информации по Хартли, передаваемое двумя сообщениями
	15
	576
	32
	256
№ 5	Преобразование давления в электрический сигнал присуще следующему эффекту: фотогальваническому пьезоэлектрическому Зеебека электромагнитной индукции
№ 6	пирозлектрическому Одномодовые или многомодовые - это параметр: акустической линии связи витой пары радиоволн оптоволокна
№ 7	Стеганография: способ передачи или хранения зашифрованной информации техника сокрытия информации раздел криптографии метод подстановочного шифрования метод перестановочного шифрования
№ 8	Как связаны ключи друг с другом в системе с открытым ключом: экзистенциально логически алгоритмически математически
№ 9	Выберите то, что используют для создания цифровой подписи: Открытый ключ получателя

Открытый ключ отправителя
Закрытый ключ получателя
Закрытый ключ отправителя
№ 10 Основными видами словарных методов типа LZ являются:
адаптивные коды
коды со скользящим окном и коды с использованием адаптивного словаря
адаптивный код Хаффмана и коды с использованием адаптивного словаря
оптимальные коды